



Assemblée parlementaire de l'OTAN

COMMISSION DES SCIENCES ET DES
TECHNOLOGIES

CYBERESPACE ET
SECURITE EURO-ATLANTIQUE

RAPPORT SPECIAL

Philippe VITEL (France)
Rapporteur spécial

TABLE DES MATIERES

I.	INTRODUCTION	1
II.	CYBERESPACE ET SECURITE NATIONALE	1
A.	LE CONTEXTE GENERAL DES CYBERMENACES	2
B.	LES CYBERMENACES CONTRE LA SECURITE NATIONALE	3
C.	LES MESURES DE PROTECTION CONTRE LES MENACES A LA SECURITE NATIONALE PROVENANT DU CYBERESPACE.....	4
1.	Cyberdéfense	4
2.	Cyberdissuasion	5
3.	Maitrise des cyberarmes.....	7
D.	LES PERSPECTIVES D'UN CYBERCONFLIT ENTRE ETATS	7
III.	LES REPONSES DEFENSIVES DE LA COMMUNAUTE EURO-ATLANTIQUE	8
A.	LES ETATS-UNIS	9
B.	LA FRANCE	11
C.	L'ALLEMAGNE	13
D.	LE ROYAUME-UNI.....	14
E.	L'ESTONIE	16
F.	L'OTAN.....	17
G.	L'UNION EUROPEENNE	19
IV.	CONCLUSION.....	21
	BIBLIOGRAPHIE	23

I. INTRODUCTION

1. En l'espace de 25 ans, le cyberspace est devenu un élément incontournable de la vie moderne. Ayant acquis une place à part entière dans l'économie mondiale, il a redynamisé la société civile dans le monde industrialisé, fait naître des révolutions dans les pays en développement et fourni aux pouvoirs publics des possibilités nouvelles d'offrir des services à leurs administrés. Toutefois, parallèlement à ces évolutions positives, le nombre de menaces s'est considérablement accru, que ce soit celles ayant lieu dans le cyberspace ou contre lui, ou les menaces rendues possibles par son existence. La criminalité et l'espionnage sont à n'en pas douter les menaces les plus courantes aujourd'hui dans le cyberspace. « Le coût de la cybercriminalité et du cyberespionnage pour l'économie mondiale se mesure probablement en centaines de milliards de dollars » (CSIS/McAfee, 2013). La subversion politique est un autre phénomène qui prend de plus en plus d'ampleur dans le cyberspace. Il est désormais possible, grâce à Internet, de mobiliser facilement des sympathisants et d'ébranler pacifiquement la confiance des populations dans un système politique ; que l'on juge la cause « légitime » ou « illégitime » dépend évidemment du point de vue de chacun.

2. Les activités criminelles, l'espionnage industriel ou les actes de subversion commis dans le cyberspace constituent rarement des menaces pour la sécurité nationale. La plupart du temps, ces actes intéressent les services responsables de l'application de la loi. Le but du présent rapport est au contraire d'examiner les cybermenaces pouvant avoir un impact direct sur la sécurité nationale. Cette catégorie de cybermenaces ne cesse d'augmenter, et les gouvernements du monde entier comme les organisations internationales se demandent comment y faire face. Nous nous intéresserons donc plus spécifiquement, dans le présent rapport, aux aspects suivants : le contexte général des cybermenaces ; les menaces spécifiques à l'encontre des forces armées et des infrastructures essentielles qui portent directement atteinte à la sécurité d'un Etat ; les mesures de protection éventuelles ; enfin, les perspectives d'un cyberconflit entre Etats. Nous examinerons ensuite les initiatives prises par cinq Etats membres de l'OTAN – les Etats-Unis, la France, l'Allemagne, le Royaume-Uni et l'Estonie – ainsi que par l'OTAN elle-même et l'Union européenne (UE), afin d'illustrer comment différents acteurs internationaux font face aux cybermenaces.

3. Le présent rapport spécial a été préparé pour la Commission des sciences et des technologies (STC) de l'Assemblée parlementaire de l'OTAN, pour servir de base à un débat transatlantique sur la nature des cybermenaces et la manière dont la cybersécurité coordonnée et collective peut améliorer la sécurité de la zone euro-atlantique. Ce projet de rapport permet en outre à son auteur de contribuer à la tenue d'un débat public éclairé et réaliste sur la question de la cybersécurité. Il fait suite à de précédents rapports de l'Assemblée sur le même thème (le rapport de la Commission de la défense et de la sécurité en 2009, *L'OTAN et la cyberdéfense*, et celui de la Commission sur la dimension civile de la sécurité en 2011, *Information et sécurité nationale*), à la résolution de l'AP-OTAN en 2011 sur la cybersécurité, ainsi qu'aux débats qui n'ont cessé d'avoir lieu sur le sujet dans le cadre des réunions et des missions de cette instance.

II. CYBERESPACE ET SECURITE NATIONALE

4. Pour comprendre comment les Etats et les organisations internationales peuvent faire face aux cybermenaces qui portent atteinte à la sécurité nationale, il est important : d'appréhender le contexte général de ces cybermenaces, y compris le mode de fonctionnement des codes informatiques malveillants ; de voir quelles sont les menaces particulières pour les forces armées et les infrastructures essentielles dans le cyberspace ; enfin, de conceptualiser les mesures de protection éventuelles. Cette section s'achève par une analyse de la faisabilité d'une véritable cyberguerre.

A. LE CONTEXTE GENERAL DES CYBERMENACES

5. Le cyberspace peut se définir comme « un espace sans frontières au sein de l'environnement de l'information, dont les caractéristiques uniques et spécifiques sont définies par l'utilisation qui est faite du spectre électronique et électromagnétique pour créer, stocker, modifier, échanger et exploiter des informations via des réseaux interconnectés et interdépendants utilisant des technologies de l'information et de la communication » (Kuehl, 2009). Il n'existe pas *un seul* cyberspace : Internet est le plus courant, mais tous les réseaux n'y sont pas connectés. On peut même dire que les réseaux les plus importants sont (ou devraient être) maintenus à l'écart d'Internet. Quoi qu'il en soit, les menaces dont ces réseaux font l'objet dans le cyberspace sont en augmentation, des acteurs potentiellement hostiles réussissant à trouver de nouveaux moyens pour y accéder.

6. Les cybermenaces à l'encontre des réseaux militaires et des infrastructures essentielles englobent toute une série d'activités qui vont de l'espionnage et du sabotage à des actes pouvant être considérés comme usage de la force voire, dans les cas extrêmes, comme des actes de guerre. Aucune cyberattaque connue n'a encore été classée dans la catégorie « usage de la force » ou « acte de guerre ». Jusqu'ici, l'écrasante majorité des atteintes à la sécurité n'ont eu aucun impact physique direct et concernaient soit des actes d'espionnage, soit des interruptions de services sur le réseau (notamment des communications). Parmi cet éventail de menaces, il est important de faire la distinction entre deux catégories de cyberactions hostiles – même si ce n'est souvent pas aisé dans la pratique. Une cyberattaque « désigne l'accomplissement d'actes délibérés visant à modifier, perturber, tromper, détériorer ou détruire les systèmes ou les réseaux informatiques utilisés par un adversaire, ou les informations/programmes qui se trouvent sur ces systèmes/réseaux ou qui y transitent » (Lin, 2012). Pour commettre une cyberattaque, il est nécessaire d'utiliser un code malveillant permettant d'exercer une menace ou de causer « des préjudices physiques, fonctionnels ou mentaux aux structures, systèmes ou êtres vivants » (Rid, 2013). De son côté, la cyberintrusion – ou simplement le cyberespionnage – « désigne l'accomplissement d'actes délibérés visant à pénétrer les systèmes ou les réseaux informatiques utilisés par un adversaire en vue de se procurer les informations qui se trouvent sur ces systèmes/réseaux ou qui y transitent » (Lin, 2012).

7. Pour être efficace, un code informatique malveillant a besoin de trois éléments : vulnérabilité, accès et charge virale (Lin, 2010). Par définition, ce code ne parvient à ses fins que s'il existe une vulnérabilité (un défaut ou un dysfonctionnement) dans le système visé. C'est là une différence clé entre les cybermenaces et les menaces classiques. Les saboteurs, les espions ou les armes qui ne relèvent pas du cyberspace n'ont pas besoin d'une défaillance rédhibitoire pour réussir ; à l'inverse, un réseau informatique qui ne présente aucune défaillance est parfaitement à l'abri d'une cyberattaque. Cela dit, compte tenu de la complexité des systèmes d'aujourd'hui, il est très peu probable, voire impossible, que les réseaux informatiques soient dépourvus de points faibles susceptibles d'être exploités par des acteurs hostiles. L'exigence de vulnérabilité admet toutefois une exception : l'attaque par déni de service, qui vise à rendre un réseau informatique indisponible, consiste non pas à exploiter un point faible mais à submerger la cible avec un trafic excessif. La deuxième exigence est l'accès de l'acteur hostile au système vulnérable. Cet accès peut se faire à distance, par exemple via la connexion du système à Internet ou à d'autres réseaux publics. Il peut aussi s'opérer de façon rapprochée : un individu « infiltré » pénètre directement dans le système et y introduit un code malveillant (par exemple, à l'aide d'une clé USB) ; autre cas de figure : un acteur extérieur trafique des composants logiciels ou matériels qui sont ensuite intégrés ou raccordés au système visé. L'acteur hostile doit, au final, insérer la « charge virale » dans le système afin qu'elle y exécute l'action malveillante souhaitée. Cette action peut être l'installation d'un logiciel de surveillance ou la destruction du système, parfois en causant indirectement la blessure des opérateurs.

8. Le caractère très spécifique des cybermenaces tient au fait qu'elles peuvent provenir d'un large éventail d'acteurs situés à tous les niveaux. Les cyberattaques ne sont pas le domaine

réservé des Etats. Bien au contraire, les obstacles à l'entrée sont peu dissuasifs pour des acteurs potentiellement hostiles. Les codes malveillants sont facilement accessibles, que ce soit auprès de sources publiques ou sur un marché noir en pleine expansion. Même si ces codes ne sont pas en libre accès, un pirate [hacker] ingénieux peut en concevoir un facilement avec peu de moyens. Les individus se livrant à des actes de cyberintrusion et à des cyberattaques contre les forces armées ou les réseaux essentiels sont notamment des pirates isolés, des « hacktivistes », des espions industriels, des organisations criminelles, des groupes terroristes, des gouvernements et des organisations internationales. Cette grande variété d'adversaires potentiels pose évidemment des défis uniques pour les pouvoirs publics. Un problème de taille est que, contrairement aux Etats, les acteurs non étatiques peuvent facilement ignorer le droit international et viser des objectifs civils, ce qui est interdit par le droit humanitaire international. Du fait du large éventail d'acteurs, les analyses comparatives montrent que les stratégies nationales de cybersécurité sélectionnent différemment les cybermenaces et les ennemis potentiels les plus importants (Robinson *et al.*, 2013). Cela dit, bien que tous ces acteurs soient capables de fomenter des cyberattaques susceptibles de provoquer de graves dommages, la plus grande inquiétude provient des cyberprogrammes offensifs financés par les Etats, dont les ressources sont bien supérieures à celles des acteurs non étatiques.

B. LES CYBERMENACES CONTRE LA SECURITE NATIONALE

9. En règle générale, une cybermenace peut représenter un danger pour la sécurité nationale lorsque les réseaux militaires ou les infrastructures essentielles sont visés. Les autres cybermenaces peuvent (et doivent) pour la plupart être gérées par les services responsables de l'application de la loi. Les systèmes des forces armées ainsi que les infrastructures essentielles présentent des caractéristiques qui les rendent de plus en plus vulnérables.

10. Dans le cas des forces armées, l'importance accordée au cyberespace (et l'utilisation qui en est faite) augmentent rapidement. Les systèmes, dispositifs et plateformes en réseau possèdent d'ores et déjà une valeur inestimable. Or, plus les forces armées utiliseront des capacités interconnectées, et plus elles s'exposeront à des attaques potentiellement dévastatrices. En vérité, la fréquence des cyberintrusions dans les systèmes militaires s'est considérablement accrue, et le développement à l'échelle mondiale de cybercapacités offensives ne cesse de progresser. A l'instar de n'importe quel réseau informatique, les systèmes militaires sont vulnérables face aux attaques provenant des réseaux eux-mêmes ou de composants logiciels/matériels susceptibles d'avoir été trafiqués avant leur raccordement auxdits systèmes. Cette menace est aggravée par le fait que la majorité des infrastructures de communication et d'information sont détenues et exploitées par des sociétés privées, et qu'un grand nombre de composants sont acquis via les chaînes d'approvisionnement mondiales. Par ailleurs, bien que les systèmes les plus sensibles soient théoriquement isolés des systèmes plus ouverts, leur porosité demeure et un acteur malveillant déterminé peut trouver des points d'accès suffisants. Les principales difficultés à cet égard sont donc d'empêcher les acteurs hostiles d'accéder aux réseaux sensibles et de garantir que les composants n'ont pas fait l'objet d'une attaque.

11. Les infrastructures essentielles, qu'elles soient gérées par l'Etat ou par des intérêts privés, sont probablement plus vulnérables aux cyberintrusions et aux cyberattaques que ne le sont les forces armées. Bien qu'il n'existe pas de définition standard de ce qu'est une infrastructure essentielle, l'expression recouvre généralement les installations et les services civils indispensables au fonctionnement de base d'une société donnée, ou dont l'absence lui serait très préjudiciable. Les secteurs souvent considérés comme essentiels sont, entre autres : administrations, énergie, transports, services financiers, alimentation, information et communications. Ces secteurs font de plus en plus l'objet de cybermenaces en raison de l'utilisation croissante des technologies de l'information pour gérer et fournir les services, ce qui élargit la surface d'attaque des infrastructures essentielles et accroît le risque d'une succession de défaillances. Les infrastructures essentielles sont particulièrement fragiles car leurs propriétaires, leurs opérateurs et leurs sous-traitants utilisent de plus en plus des logiciels ou matériels en accès

libre (tels que les téléphones portables ou les tablettes), ainsi que des réseaux publics (en association avec des réseaux privés, ou en lieu et place de ces derniers). La question est particulièrement préoccupante pour ce qui est des systèmes de contrôle industriel, par exemple les systèmes d'acquisition et de contrôle de données (*Supervisory Control and Data Acquisition*, SCADA). Ces systèmes sont généralement intégrés à des réseaux isolés. Or, dans la mesure où les réseaux plus ouverts promettent toutes sortes de possibilités nouvelles (comme par exemple une plus grande efficacité), ces systèmes sont de plus en plus raccordés à ces autres réseaux. Toutes ces évolutions accentuent la vulnérabilité des infrastructures essentielles et augmentent l'impact éventuel d'une cyberattaque réussie.

12. La grande difficulté pour mettre en œuvre une stratégie efficace en matière de protection des infrastructures essentielles contre les cybermenaces est de trouver un moyen permettant de gérer au mieux les relations public-privé entre, d'un côté l'Etat, et de l'autre, les propriétaires et opérateurs desdites infrastructures. Les mesures incitatives mis en œuvre diffèrent sensiblement entre les deux parties : les pouvoirs publics sont surtout préoccupés par la sécurité, alors que les entreprises privées ont les yeux rivés sur leurs résultats financiers. Les gouvernements nationaux et les organisations internationales ont le choix entre la mise en place de normes facultatives en matière de cybersécurité, l'adoption de réglementations contraignantes ou la poursuite d'une politique hybride associant ces deux options. Compte tenu de la rapidité à laquelle les technologies de l'information évoluent et progressent, aucune de ces options n'est facile à mettre en œuvre.

C. LES MESURES DE PROTECTION CONTRE LES MENACES A LA SECURITE NATIONALE PROVENANT DU CYBERESPACE

13. Les Etats disposent d'un certain nombre d'options pour lutter contre les menaces cybernétiques à la sécurité nationale. Ils ont le choix, en l'occurrence, entre la cyberdéfense, la cyberdissuasion et la maîtrise des cyberarmes.

1. Cyberdéfense

14. Le premier rempart contre les cybermenaces est la cyberdéfense, qui empêche des acteurs hostiles d'opérer avec succès des cyberintrusions, ou tout au moins d'en tirer profit. Les gouvernements et les entités privées peuvent prendre des mesures préventives et passives. Les Etats peuvent améliorer leur connaissance de ce qu'est une cybermenace et investir dans la recherche-développement de technologies permettant d'améliorer la cybersécurité. Quant aux organisations, elles peuvent créer des mesures incitatives pour amener les opérateurs et les clients à respecter les consignes élémentaires en matière de cybersécurité (Lin, 2012). Le personnel peut par exemple être formé à la cyber « hygiène » ; des audits peuvent être réalisés pour vérifier et évaluer les comportements ; enfin, des récompenses peuvent être attribuées pour améliorer le respect des consignes. Du point de vue technique, la cyberdéfense consiste surtout à remédier aux vulnérabilités des systèmes, par exemple en corrigeant un logiciel défaillant, en fermant des voies d'accès (à l'aide d'un pare-feu, par exemple), et en neutralisant la charge virale, y compris lorsque l'intrusion a réussi (par exemple en rendant les fichiers sensibles inutilisables, que ce soit par cryptage ou tout autre procédé). Des « *pots à miel* » – c'est-à-dire des leurres permettant d'éloigner les intrus des informations véritablement utiles – peuvent être installés, de même que des logiciels capables de détecter et de surveiller les intrusions. Pour empêcher que les cyberattaques ne causent des dommages intolérables, les Etats peuvent aussi veiller à une meilleure continuité des systèmes en renforçant leur redondance et leur résilience, et en améliorant leur propre capacité à réparer et remettre en état les systèmes ayant été la cible d'une attaque.

15. La notion de cyberdéfense active suscite une grande attention. Les techniques de cyberdéfense préventive et passive susmentionnées sont essentiellement réactives : les

organisations essaient de réduire les vulnérabilités, de bloquer les points d'accès et de minimiser la capacité de destruction de la charge virale. Le problème est que les auteurs de cyberintrusions sont déterminés, qu'ils sont probablement beaucoup plus habiles que les cyber-défenseurs, et qu'ils sont capables de s'adapter rapidement pour déjouer les nouveaux procédés de cyberdéfense. Les techniques de cyberdéfense active permettent à ceux qui les mettent en œuvre de mettre au jour, de définir, d'analyser et d'atténuer les cybermenaces en temps réel. Les organisations peuvent par exemple engager une « poursuite immédiate » à l'encontre des intrus, c'est-à-dire « pirater en riposte » leurs réseaux, que ce soit ouvertement ou en douce. Néanmoins, bien que ces défenses actives présentent de nombreux avantages, leurs incidences pratiques et juridiques ne sont pas encore très claires, en particulier pour les acteurs étatiques (Farwell et Rohozinski, 2012). Dans quelles circonstances "le piratage de riposte" constitue-t-il une cyberagression injustifiée ? Qui a autorité pour exercer une défense active et dans quelles circonstances ? Où se trouve la frontière entre une défense active et une attaque préventive ? Telles sont quelques-unes des questions qui restent sans réponse.

2. Cyberdissuasion

16. Un grand nombre d'experts et de responsables gouvernementaux estiment qu'aujourd'hui ce sont les attaquants qui ont l'avantage dans le cyberspace, et que cela n'est pas prêt de changer. Les cyberdéfenses seraient par conséquent insuffisantes pour empêcher d'éventuels pirates de pénétrer dans les infrastructures essentielles et aux réseaux militaires. Des acteurs hostiles, doués et ingénieux trouveront toujours un moyen de déjouer les cyberdéfenses. Ce point de vue va souvent de pair avec la conviction que les cyberattaques peuvent causer des dommages considérables en un rien de temps. Un grand nombre d'experts et, à vrai dire, de gouvernements se tournent donc vers des stratégies de dissuasion axées sur la sanction, en d'autres termes, des stratégies visant à dissuader les pirates de commettre des cyberattaques en les menaçant de sérieuses représailles. Ces actions de représailles ne sont pas nécessairement circonscrites au cyberspace, mais le recours à des cybercapacités offensives serait certainement utile dans ces stratégies de dissuasion.

17. Avant de décrire ce que pourrait être une stratégie de cyberdissuasion et à quels problèmes elle pourrait se heurter, il est important de noter qu'un nombre grandissant d'analystes n'ont pas un avis aussi tranché sur les cyberattaques et mettent en garde contre l'utilisation excessive de la cyberdissuasion. Ils avancent que la meilleure défense reste une bonne défense. Les cyberarmes sophistiquées – donc plus dangereuses – nécessitent de grandes compétences pour être développées, et elles doivent ensuite être adaptées à chacune de leur cible. Par ailleurs, les dommages qu'elles peuvent causer sont souvent incertains, imprévisibles, voire souvent contraires au but recherché. Il est donc vraisemblable que ces dommages ne soient finalement que peu importants et très ciblés. Plus les cyberarmes sont sophistiquées, plus les possibilités de stopper l'attaquant sont grandes. Par conséquent, comme l'indiquent les analystes, trop s'appuyer sur la cyberdissuasion pourrait créer un sentiment de fausse sécurité et même avoir des effets déstabilisateurs dans les rapports avec un éventuel adversaire.

18. Malgré ces appels à la prudence, de nombreux Etats élaborent ou mettent en œuvre des stratégies de dissuasion. Il est donc impératif de comprendre les complexités et les implications de la cyberdissuasion qui, malgré ses nombreuses similitudes avec les formes de dissuasion classiques, présente également des différences notables du fait de la nature du cyberspace. Trois difficultés sont à noter en particulier : l'attribution de l'attaque ; la fixation éventuelle d'un seuil de représailles ; enfin, la proportionnalité de la menace de représailles.

19. Il est très difficile, dans le cyberspace, de remonter jusqu'à l'auteur et/ou instigateur d'une intrusion : c'est ce que l'on appelle le problème de l'attribution de l'attaque. D'une part, la plupart des intrusions ont lieu via des réseaux tiers, le plus souvent par l'intermédiaire de « botnets » (ou ordinateurs zombies), c'est-à-dire un réseau d'ordinateurs appartenant à des personnes qui ne sont pas au courant que leurs machines sont utilisées à des fins malveillantes. D'autre part, même

si l'on réussit à retrouver la trace des auteurs d'une attaque dans un pays donné, il est très difficile d'établir un lien entre ces auteurs et un Etat (les pirates ne logent pas nécessairement dans une caserne ni ne portent d'uniforme). Il est fréquent que ce lien n'existe même pas. En fait, une cyberintrusion peut être le fait de ceux que l'on surnomme les « pirates patriotes », des individus qui veulent apporter un soutien à un Etat, mais qui n'agissent pas en son nom. Comme l'indique un observateur : « L'attribution d'une attaque est difficile, voire impossible, si son auteur (Etat ou individu) : utilise les outils et techniques modernes et ne laisse aucune trace ; assure une sécurité opérationnelle parfaite ; ne formule aucune exigence ; et surtout, entreprend une action hostile qui requiert une réaction rapide. » (Lin, 2012). En revanche, d'autres observateurs dont le gouvernement des Etats-Unis sont optimistes quant aux progrès qui seront accomplis au regard de l'attribution des attaques, et rendront ainsi la dissuasion possible. D'ailleurs, l'attribution des attaques n'est peut-être pas aussi ardue que beaucoup le prétendent. Plus une cyberattaque est grave, et plus son auteur a intérêt à en revendiquer la responsabilité (Rid, 2013). Si l'objectif d'une attaque est d'exercer une contrainte ou une pression sur l'adversaire, l'attribution est nécessaire : en effet, comment la victime peut-elle satisfaire aux exigences de l'attaquant si elle ne sait pas qui il est ? Si l'attaque est commise dans le cadre d'un conflit armé, la victime connaît vraisemblablement son auteur.

20. Un autre problème de base de la cyberdissuasion est la question de la fixation éventuelle d'un seuil de représailles. Toutes les cyberattaques ne méritent pas des représailles. Dans les cas de cyberespionnage, par exemple, la menace de représailles n'est pas crédible car l'ordre international n'interdit pas l'espionnage entre Etats. Si un Etat est clairement victime d'une cyberattaque, la question qui se pose est de déterminer quel degré et quel type de dommage justifient des représailles. Peut-on fixer un seuil de représailles en fonction du préjudice économique, des dégâts physiques causés aux infrastructures ou des pertes en vies humaines (dans la mesure où ces pertes sont uniquement une conséquence indirecte et parfois involontaire de l'attaque) ? Il n'existe à ce stade aucune interprétation juridique claire de ce qui constitue un usage de la force – voire un acte de guerre – dans une cyberattaque. En l'absence d'une telle interprétation, comment peut-on fixer un seuil de représailles ? Et si ce seuil est fixé, peut-il encourager un adversaire potentiel à mener des actions juste en dessous du seuil, pour ne pas avoir à craindre des représailles ?

21. Une troisième difficulté tient à la proportionnalité des représailles. Tout d'abord, les représailles doivent-elles avoir lieu uniquement dans le cyberspace, ou s'exercer d'une autre manière ? La réponse est que cela dépend évidemment de la gravité de l'acte commis. Cela dit, si les représailles doivent avoir lieu dans le cyberspace, est-il envisageable que la victime menace les actifs de l'attaquant (Libicki, 2009) ? Le cyberspace regorge d'acteurs hostiles et, dans la mesure où les cyber-représailles doivent être adaptées à la gravité de l'attaque ainsi qu'aux vulnérabilités respectives, une multitude d'efforts et de ressources sont nécessaires pour adopter une position dissuasive crédible. Par ailleurs, même si un Etat conçoit des mesures de représailles spécifiques, il n'est pas sûr que l'agresseur soit toujours vulnérable au moment où les représailles s'avèreraient nécessaires.

22. La cyberdissuasion est complexe, et de nombreuses questions restent encore sans réponse. Les Etats ou les organisations peuvent-ils raisonnablement étendre la cyberdissuasion à leurs alliés ? Quels actes de représailles conduiraient à l'escalade involontaire d'un conflit ? Toutes ces questions trouveront probablement une réponse en temps voulu. Après tout, il a fallu près de 20 ans aux stratèges "de l'atome" pour tirer des enseignements fondamentaux sur ce que voulait dire la dissuasion à l'époque du nucléaire. De nombreux experts laissent toutefois entendre qu'à ce stade, « l'ambiguïté stratégique » et la souplesse – concernant les types d'actes entraînant des représailles et quelle forme doivent prendre ces représailles – est la position la plus acceptable en matière de cyberdissuasion. Cela dit, à mesure que le nombre de cyberattaques augmentera et que la dissuasion sera mise à l'épreuve, cette position pourrait être mise à mal.

3. Maîtrise des cyberarmes

23. Une certaine forme de maîtrise des cyberarmes (via la mise en place de normes et de mesures juridiques internationales, par exemple) pourrait être une solution pour atténuer les menaces à la sécurité nationale provenant du cyberspace. Si la cyberdéfense et la cyberdissuasion suscitent déjà de nombreuses questions, cela est encore plus vrai pour ce qui est de la maîtrise des cyberarmes. En fait, les possibilités de trouver des réponses à ces questions et de mettre en place une maîtrise des cyberarmes, fussent-elles rudimentaires, semblent faibles pour le moment (Lin, 2012). Si l'on s'oriente vers une restriction de la recherche-développement des codes malveillants, comment pourra-t-on vérifier qu'aucun acteur – étatique ou non – ne développe un tel code ? Après tout, il suffit, pour rédiger un code, d'un pirate intelligent doté d'un minimum d'équipement. Par ailleurs, l'une des méthodes les plus efficaces pour détecter des défaillances sur les réseaux est de procéder à un test de pénétration, à savoir, déployer un simulacre d'adversaire pour tenter de mettre à mal les systèmes de défense à l'aide d'un code malveillant. L'interdiction d'une telle activité signifierait que les acteurs hostiles seraient clairement avantagés. Si l'on restreint ou interdit l'utilisation de codes malveillants par les pays qui sont en conflit, ces pays seraient-ils tentés de les utiliser malgré tout, si, dans ce conflit, ils n'avaient pas le dessus, et qu'est-ce qui empêcherait des acteurs non étatiques (par exemple des terroristes ou des « pirates patriotes ») d'utiliser lesdits codes ? Si l'on devait proscrire le cyberespionnage, cela irait bien au-delà du régime international actuel, dans lequel l'espionnage n'est pas considéré comme une activité interdite. Cela dit, des recherches plus poussées concernant la maîtrise des cyberarmes pourraient donner naissance à des approches novatrices et accroître les perspectives de réussite. L'adoption, en parallèle, d'une vision commune sur les concepts du cyberspace pourrait également être utile. Enfin, la signature d'accords sur les problèmes du cyberspace qui dépassent la sphère de la sécurité nationale (la cybercriminalité, par exemple) pourrait ouvrir de nouvelles voies dans la maîtrise des cyberarmes. Pour l'heure cependant, les Etats doivent s'accommoder d'un monde dans lequel les codes malveillants continueront à proliférer.

D. LES PERSPECTIVES D'UN CYBERCONFLIT ENTRE ETATS

24. Compte tenu des vulnérabilités actuelles des réseaux militaires et des infrastructures essentielles, mais aussi de l'intense prolifération des cybercapacités offensives, existe-t-il un véritable risque de cyberconflit entre Etats ? Malgré une tendance parfois forte à l'exagération au sein de l'opinion publique, il existe de bonnes raisons d'être sceptique.

25. Premièrement, les cyberarmes ne causent des dommages physiques (au matériel, aux infrastructures ou aux personnes) que de manière indirecte, en provoquant le dysfonctionnement des systèmes. Jusqu'ici, l'utilisation de codes malveillants n'a causé en fait que trois cas connus¹ de dommages physiques, et aucun d'eux n'a eu de conséquences sur des vies humaines : en 2007, le test de pénétration « Aurora » mené dans un laboratoire a causé de sérieux dégâts sur un générateur ; l'utilisation du ver informatique Stuxnet à des fins de sabotage a provoqué la destruction de centrifugeuses iraniennes ; en 2012, le virus Shamoon utilisé à l'encontre de la société saoudienne Aramco (*Saudi Arabian Oil Company*) a causé de graves dégâts à son réseau interne (mais aucun, il faut le noter, à ses infrastructures gazières et pétrolières). Deuxièmement, les cyberattaques doivent être soigneusement adaptées à chacune de leur cible, ce qui veut dire que les cyberarmes ont peu de chances d'être déployées dans le cadre d'attaques de grande ampleur. Troisièmement, une fois qu'une cyberarme est lancée, il est très peu probable qu'elle soit réutilisée à des fins similaires. En vérité, il y a plus de chances qu'elle soit bloquée, vu que la victime de l'attaque s'adapte au code malveillant. Quatrièmement, bien que la valeur d'un code diminue aux yeux de l'attaquant une fois qu'il l'a utilisé, d'autres acteurs – la victime elle-même ou des tiers – peuvent modifier ce code sophistiqué et l'utiliser contre l'attaquant. Enfin, une fois

¹ Le rapporteur suppose que d'autres cas, peut-être plus graves, se sont produits, mais qu'ils n'ont pas été rendus publics.

lancée, une cyberarme peut échapper à tout contrôle et frapper des cibles de manière accidentelle, voire des cibles se trouvant dans le pays d'où provient l'attaque.

26. Pour toutes ces raisons, la plupart des analystes conviennent aujourd'hui qu'il y a peu de risques pour que les cyberarmes causent en l'espace de très peu de temps des dommages considérables aux effets stratégiques indéniables comme une frappe nucléaire de neutralisation). Cela ne veut pas dire que les cyberarmes ne trouveront pas une place dans les conflits et dans la façon dont ils sont menés, mais « qu'elles doivent simplement être considérées comme une catégorie d'armes parmi d'autres » (Gray, 2013). Les risques de cyberterrorisme ne doivent pas être sous-estimés, mais là aussi, la prudence est de mise car les terroristes s'orientent généralement vers des cibles très visibles et présentant une grande dimension émotionnelle, qui sont difficiles à atteindre avec des cyberarmes. Du point de vue des Etats, les cyberarmes possèdent bel et bien des avantages uniques : elles peuvent atteindre des objectifs militaires plus rapidement, sur une plus longue portée et de façon plus économique, moins risquée et plus furtive (Gray, 2013 ; Bockel, 2012). Pour les experts militaires, les cyberattaques pourraient jouer le rôle de facilitateurs des actions militaires, notamment en provoquant un effet de surprise susceptible de conduire à un succès opérationnel – par exemple au début d'un conflit armé de grande ampleur ou lors d'opérations spéciales (Libicki, 2009). Un grand nombre de juristes et de gouvernements estiment également que les cyberarmes ne posent aucun problème de fond au regard du droit des conflits armés, même si, s'agissant des cyberattaques, ce dernier doit être interprété. En d'autres termes, comme le résument deux observateurs : « L'organisation type des conflits survenant à l'ère de l'information n'est pas un « cyberconflit » entre Etats qui se déroule uniquement en ligne et dans lequel les objectifs stratégiques peuvent être atteints au moyen d'opérations coup de main menées dans le cyberspace. L'organisation type est en revanche une « cyberéchauffourée », c'est-à-dire un fond plus ou moins constant d'activité de faible intensité dans un vaste « paysage virtuel », souvent menée par des acteurs différents et sans aucune conséquence stratégique (ou si peu), quelle que soit l'importance globale de ces enjeux. » (Betz et Stevens, 2011).

III. LES REPONSES DEFENSIVES DE LA COMMUNAUTE EURO-ATLANTIQUE

27. Compte tenu de l'impact éventuel des cybermenaces et de leur prolifération à l'échelle mondiale, les Etats de la communauté euro-atlantique envisagent de mettre au point et d'encourager une politique et des pratiques en matière de cybersécurité aux niveaux national et multinational. Bien que la question de la cybersécurité ait bénéficié ces dernières années d'une attention soutenue à un niveau élevé, les mesures de protection contre les cybermenaces tardent encore à se mettre en place. Pour illustrer les efforts mis en œuvre dans le domaine de la cybersécurité, nous examinerons tout d'abord dans la présente section les actions engagées par les Etats-Unis (considérés comme le leader de la communauté euro-atlantique en matière de cybersécurité) la France, l'Allemagne et le Royaume-Uni, les trois pays européens possédant le plus gros budget de la défense au sein de l'OTAN, ainsi que l'Estonie, à la pointe des efforts poursuivis en matière de la cybersécurité après les attaques dont elle a été victime en 2007. Nous nous intéresserons ensuite aux initiatives multinationales et à l'action innovante de l'UE et de l'OTAN en matière de conception et de mise en œuvre de mesures de protection. Ces deux organisations cherchent à élaborer des politiques globales comportant des normes claires sur la sécurité des réseaux, et mettent l'accent sur l'importance de la coopération entre les gouvernements nationaux et le secteur privé. Les principales différences entre les politiques de l'UE et de l'OTAN en matière de cybersécurité sont davantage dues au rôle différent des deux organisations qu'à leur approche divergente de la cybersécurité. L'OTAN possède ses propres réseaux et systèmes informatiques. Au sein de l'UE, les responsabilités en matière de cybersécurité incombent principalement aux Etats membres pour leurs réseaux et systèmes nationaux, tandis que les institutions européennes sont responsables de leurs propres équipements (Robinson, 2013).

28. Dans la mesure où les doctrines et les règles d'engagement d'une cyberaction offensive sont classifiées "secret", la présente section ne s'intéressera pas spécifiquement aux cybercapacités offensives. La France, le Royaume-Uni et les Etats-Unis ont fait savoir qu'ils détenaient ce type de cybercapacités ; en revanche l'OTAN et l'UE, en tant qu'organisations internationales, en sont dépourvues. Nous éviterons également dans cette section d'examiner en détail les mesures de maîtrise des cyberarmes. Pour un certain nombre de raisons, les pays décrits ci-après ne sont globalement pas favorables à la mise en place de règles formelles sur la maîtrise des cyberarmes, mais ils ne refusent pas le débat sur les mesures à prendre pour instaurer la confiance, les normes à respecter et la conduite à tenir à cet égard.

A. LES ETATS-UNIS

29. La stratégie de sécurité nationale élaborée en 2010 présente les cybermenaces comme « l'un des plus grands défis pour la sécurité nationale, la sûreté publique et l'économie » auxquels sont confrontés les Etats-Unis (Maison-Blanche, 2010). En fait, malgré la baisse générale des dépenses militaires, le ministère de la Défense a fait de la cybersécurité l'une de ses priorités dans le cadre des projections budgétaires actuelles (Serbu, 2014). Depuis 2009, le budget américain de la cybersécurité s'est accru, en moyenne, de 0,27 % par an (Joubert, 2014). La stratégie américaine dans le domaine de la cybersécurité vise deux grands objectifs : améliorer la résilience aux cyberincidents et réduire la cybermenace. Le premier de ces objectifs nécessite un renforcement de l'infrastructure numérique, une amélioration des méthodes de défense et une aide à la récupération rapide en cas de cyberincidents. Quant au second, il requiert « l'élaboration – en collaboration avec les alliés, de normes internationales relatives aux comportements admis dans le cyberspace, le renforcement des capacités des services chargés de l'application de la loi en matière de lutte contre la cybercriminalité, ainsi qu'une action de dissuasion à l'égard des adversaires potentiels afin qu'ils n'exploitent pas les vulnérabilités restantes » (Maison-Blanche, 2010).

30. D'un point de vue organisationnel, la tâche de protection de l'infrastructure numérique est répartie aux Etats-Unis entre le département de la Défense (DoD - *Department of Defense*), qui assure la sécurité des réseaux militaires, et le département de la Sécurité intérieure (DHS – *Department of Homeland Security*) qui sécurise les réseaux publics civils et coopère avec les entités privées.

31. Au sein du DoD, les responsabilités concernant le cyberspace sont confiées au Cybercommandement (USCYBERCOM), installé dans les locaux de l'Agence de sécurité nationale (NSA), chargée du recueil des renseignements d'origine électromagnétique. Le directeur de la NSA possède en fait « deux casquettes », puisqu'il est aussi commandant de l'USCYBERCOM. Ce dernier a pour tâche de synchroniser et de coordonner les actions de sécurisation du cyberspace entre les différentes divisions de l'armée américaine. De manière générale, le DoD s'occupe de trois types de cyberattaques : le vol ou l'exploitation de données ; l'interruption ou le déni d'accès ou de service sur les réseaux et les systèmes ; les actes à visée destructrice.

32. La politique actuelle du DoD au regard du cyberspace s'appuie sur la stratégie de conduite des opérations dans le cyberspace, mise au point en 2011. Cette stratégie décrit le contexte stratégique des cybermenaces et propose cinq initiatives (Département de la Défense des Etats-Unis, 2011) :

- aborder le cyberspace comme un champ d'opération requérant des tâches d'organisation, de formation et d'équipement, afin que le DoD puisse exploiter pleinement le potentiel des réseaux et des systèmes du cyberspace ;
- utiliser de nouveaux concepts opérationnels en matière de défense afin de protéger les réseaux et les systèmes du DoD ;

- collaborer avec d'autres ministères et organismes publics américains ainsi qu'avec le secteur privé, afin de mettre en œuvre une stratégie de la cybersécurité englobant toutes les instances gouvernementales ;
- nouer des relations solides avec les alliés et partenaires internationaux des Etats-Unis dans le but de renforcer la cybersécurité collective ;
- tirer parti des talents nationaux, à savoir une main-d'œuvre extrêmement qualifiée dans le domaine du cyberspace et des innovations technologiques rapides.

33. Aux Etats-Unis, la protection des infrastructures essentielles contre les cybermenaces incombe maintenant au pouvoir exécutif, le Congrès n'étant pas parvenu depuis 2002 à adopter quelque législation importante que ce soit sur la cybersécurité. Le DHS est le principal organe gouvernemental chargé de la protection des infrastructures essentielles, y compris contre les cybermenaces. Compte tenu du nombre considérable de propriétaires et d'opérateurs d'infrastructures essentielles – publiques ou privées –, le rôle joué par le DHS est relativement vaste. En l'occurrence, ce département formule « des orientations stratégiques à l'intention des partenaires publics et privés, met en avant l'harmonisation des efforts à l'échelle nationale et coordonne l'ensemble des actions fédérales visant à promouvoir la sécurité et la résilience des infrastructures essentielles du pays » (Département américain de la Sécurité intérieure, non daté).

34. Au sein du DHS, la protection des infrastructures essentielles contre les cybermenaces est coordonnée par le *National Cybersecurity and Communications Integration Center* (NCCIC). Ce centre a pour mission de favoriser la coopération et la mise en commun des informations entre tous les échelons du gouvernement et le secteur privé. L'une de ses activités consiste à effectuer un travail de sensibilisation sur les vulnérabilités, les intrusions, les incidents, les mesures d'atténuation et les actions de récupération des données. Le NCCIC assure par exemple la gestion de la *United States Computer Emergency Readiness Team* (CERT), qui intervient en cas de cyberincidents, fournit une assistance technique aux opérateurs et diffuse des notes concernant les menaces actuelles et potentielles². Bien qu'il travaille en liaison étroite avec les propriétaires et opérateurs d'infrastructures essentielles, le NCCIC n'est pas habilité à faire respecter les mesures de cybersécurité auprès du secteur privé.

35. Outre le rôle joué par le DHS, un décret-loi signé en 2013 par le président Obama, dans le but d'améliorer la cybersécurité des infrastructures essentielles, a confié au *National Institute of Standards and Technology* la tâche de créer un cadre pour la cybersécurité. Achievé en février 2014, ce cadre comporte un ensemble de normes minimales non obligatoires qui fournissent aux opérateurs privés des données de référence en matière de cybersécurité. Il pourra servir de base à la réglementation future des différents secteurs. En effet, des agences fédérales ont réalisé une évaluation des règles de cybersécurité en vigueur dans les secteurs placés sous leur responsabilité, avec la possibilité d'élaborer des normes réglementaires (Romm, 2014). La mise en œuvre du cadre précité dans tous les secteurs où il existe des infrastructures essentielles est peu probable sans une action du Congrès. Certains observateurs perçoivent toutefois, dans l'activité récente des législateurs, une volonté accrue de faire adopter divers projets de loi sur la cybersécurité. La session inter-régime du Congrès, la période située entre les élections du Congrès de 2014 et le début de la session de 2015, pourrait être cruciale pour parachever avant la fin de l'année la législation sur la cybersécurité et la protection des données (Krayem, Savelief, Davenport, et Martin, 2014). En juillet 2014, la Chambre des représentants a adopté trois textes relatifs à la protection des infrastructures essentielles. La première de ces lois, qui concerne la cybersécurité et la protection des infrastructures essentielles à l'échelle nationale, privilégie le renforcement de l'autorité du DHS, en mettant en place de façon codifiée des équipes *Cyber*

² Une CERT est une équipe d'experts intervenant rapidement en cas d'incidents liés à la sécurité informatique. Ces experts fournissent les services nécessaires pour résoudre le problème et gérer les conséquences. La plupart des CERT fournissent en outre des services de sensibilisation et de prévention, par exemple en surveillant l'environnement. Tous les membres de l'Alliance et de l'UE sont invités à se doter d'une CERT nationale. La CERT-EU vient en aide aux institutions de l'UE.

Incident Response Teams et souligne la nécessité de travailler en collaboration avec le secteur privé. La deuxième loi, qui traite de l'intensification de la recherche-développement sur les infrastructures essentielles, accroît les responsabilités du DHS en ce qui concerne la protection des infrastructures essentielles, en demandant à ce département de concevoir et de mettre à jour un plan de R-D sur les technologies de la cybersécurité. Enfin, la troisième loi, qui porte sur le personnel responsable de la cybersécurité intérieure, charge le secrétaire d'Etat à la Sécurité intérieure de mettre au point une stratégie pour former et recruter une main-d'œuvre spécialisée dans la cybersécurité intérieure (Fagan, Hertling et Dantiki, 2014).

36. Les Etats-Unis, pour qui la collaboration internationale est le premier principe à suivre pour élaborer une politique sur le cyberspace, ont publié en 2011 une stratégie internationale pour le cyberspace (Maison-Blanche, 2011). Le principal objectif de cette stratégie est de promouvoir « des infrastructures d'information et de communication ouvertes, interopérables, sûres et fiables » en créant « un environnement dans lequel des normes aux fins d'un comportement responsable orientent les actions des Etats, assurent la viabilité des partenariats et favorisent l'Etat de droit dans le cyberspace. »

B. LA FRANCE

37. En France, la cybersécurité est apparue comme un domaine spécifique de la sécurité nationale dans le Livre blanc sur la défense et la sécurité nationale de 2008. Depuis cette date, le pays n'a cessé d'améliorer ses politiques en matière de cyberdéfense et de cybersécurité, et a encore intensifié ses efforts sous l'impulsion de l'actuel ministre de la Défense, Jean-Yves Le Drian.

38. En 2009, la France a créé l'Agence nationale de la sécurité des systèmes d'information (ANSSI), placée sous la responsabilité du secrétaire général de la défense et de la sécurité nationale. L'ANSSI est à ce jour l'autorité nationale chargée de la protection des réseaux et des systèmes d'information dans les secteurs tant public que privé. Les tâches de veille, d'analyse et de réaction aux attaques commises sur des systèmes militaires sont assurées par le Centre d'analyse de lutte informatique défensive, désormais installé dans les mêmes locaux. La mission de l'ANSSI a quatre volets (ANSSI, 2013) :

- « détecter et réagir au plus tôt en cas d'attaque informatique, grâce à un centre de détection chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre de mécanismes de défense adaptés aux attaques ;
- prévenir la menace, en contribuant au développement d'une offre de produits de très haute sécurité ainsi que de produits et services de confiance pour les administrations et les acteurs économiques ;
- jouer un rôle de conseil et de soutien aux administrations et aux opérateurs des infrastructures d'importance vitale ;
- informer régulièrement le public sur les menaces, notamment par le site Internet gouvernemental de la sécurité informatique, lancé en 2008, qui a vocation à être le portail Internet de référence en matière de sécurité des systèmes d'information ».

39. Le rôle de conseil et de soutien auprès des opérateurs des infrastructures d'importance vitale qui a été attribué à l'ANSSI est rendu possible grâce aux autres volets de sa mission. Le partage d'informations, la recherche-développement et l'évaluation des risques sont des aspects clés d'un partenariat public-privé efficace dans le domaine de la cybersécurité. Ces efforts représentent le fondement de la stratégie de la France en matière de cybersécurité, et le gouvernement français est déterminé à en faire encore plus pour la protection de ses infrastructures essentielles. Dans le cadre de cet objectif, l'ANSSI a publié en 2014, en coordination avec les parties prenantes de l'industrie, des propositions concernant la classification des infrastructures d'importance vitale et l'amélioration de leur résilience aux cyberattaques. Ces

propositions serviront de base à l'élaboration d'une loi sur la cybersécurité (Drinkwater, 2014).

40. Etant de plus en plus la cible d'opérations de cyberespionnage, la France cherche à renforcer ses capacités de défense (prévention, détection et résilience) face aux cyberattaques. Répondant à ces objectifs, le Livre blanc de 2013 sur la défense et la sécurité nationale met l'accent sur le soutien de l'Etat aux compétences scientifiques et technologiques de haut niveau, le contrôle des chaînes d'approvisionnement des systèmes de sécurité et des prestataires de services, le renforcement des capacités en matière de renseignement et la coopération avec des partenaires étrangers de confiance (République française, 2013). La mise en œuvre de ces dispositions va bon train car le gouvernement est convaincu de l'urgence du sujet. En février 2014, le ministre de la Défense, Jean-Yves Le Drian, a annoncé le lancement du "Pacte Défense Cyber", doté d'un budget de 1 milliard d'euros dont les six axes sont :

- durcir le niveau de sécurité des systèmes d'information et les moyens de défense et d'intervention du ministère et de ses grands partenaires de confiance ;
- préparer l'avenir en intensifiant l'effort de recherche tant technique et académique qu'opérationnel, tout en soutenant la base industrielle ;
- renforcer les ressources humaines dédiées à la cyberdéfense et construire les parcours professionnels associés ;
- développer en Bretagne le Pôle d'excellence en cyberdéfense au profit du ministère de la défense et de la communauté nationale de cyberdéfense ;
- cultiver un réseau de partenaires étrangers, tant en Europe qu'au sein de l'Alliance atlantique et dans les zones d'intérêt stratégique ;
- favoriser l'émergence d'une communauté nationale de cyberdéfense en s'appuyant sur un cercle de partenaires et les réseaux de la réserve.

41. L'une des actions concrètes qui émergent du "Pacte Défense Cyber" est que les effectifs du Pôle d'excellence en cyberdéfense en Bretagne seront quasiment doublés (de 250 à environ 450) en l'espace de quelques années. Cela signifie que la France est en train de se rapprocher des autres acteurs européens en ce qui concerne les compétences en matière de cyberdéfense. Une autre innovation récente au niveau des institutions de l'Etat est la création d'un poste de « cyberpréfet » au ministère de l'Intérieur. Le cyberpréfet sera chargé de coordonner le plan d'action du ministère sur le renseignement économique, qui vise à protéger les industries françaises contre le cyberespionnage.

42. Le Livre blanc de 2013 sur la défense et la sécurité nationale a également pour objectif de moderniser et de renforcer la cyberdéfense française à l'égard des infrastructures essentielles, à l'heure où l'Etat vise à instaurer une réglementation centralisée. Faisant référence aux opérateurs des systèmes d'information d'importance vitale, le document précise que « l'Etat fixera, par un dispositif législatif et réglementaire approprié, les standards de sécurité à respecter à l'égard de la menace informatique et veillera à ce que les opérateurs prennent les mesures nécessaires pour détecter et traiter tout incident informatique touchant leurs systèmes sensibles » (République française, 2013). La France a donc récemment adopté, dans la loi de programmation militaire pour 2014-2020, des dispositions bien précises incluant des normes en matière de cybersécurité applicables plus particulièrement aux réseaux publics et aux opérateurs des infrastructures essentielles privées. Conformément au Livre blanc de 2013, la nouvelle loi énonce quatre principes novateurs concernant la cybersécurité des opérateurs d'importance vitale (OIV). L'ANSSI :

- peut fixer des règles de sécurité obligatoires pour les systèmes essentiels des OIV ;
- doit être informée des incidents qui se produisent sur les systèmes essentiels des OIV ;
- peut demander des contrôles de sécurité ;
- peut demander des mesures spécifiques en cas de crises majeures.

C. L'ALLEMAGNE

43. En février 2011, le gouvernement fédéral allemand a adopté une stratégie nationale sur la cybersécurité. La même année, le pays a ajouté aux lignes directrices de sa politique de défense un volet relatif à la cyberdéfense et la cybersécurité, en indiquant que les cyberattaques constituent « une menace asymétrique aux conséquences graves » (Ministère fédéral allemand de la Défense, 2011). Dans le domaine de la cyberdéfense, les menaces jugées les plus dangereuses par l'Etat allemand sont le terrorisme, les activités criminelles et la guerre, les catastrophes naturelles, la défaillance technique ou l'erreur humaine (Robinson *et al.*, 2013).

44. La stratégie de l'Allemagne en matière de cybersécurité insiste en particulier sur la nécessité de protéger les infrastructures essentielles d'information, de renforcer la cybersécurité des réseaux de l'administration publique, de mettre en place un contrôle efficace des infractions commises dans le cyberspace, et de conclure des partenariats au sein de l'Europe et à l'échelle mondiale pour mieux coordonner la cybersécurité. Cette stratégie met en fait l'accent sur le fait que la cybersécurité requiert des efforts à la fois au niveau national et avec les partenaires internationaux. Par ailleurs, compte tenu du défi commun que représentent les cybermenaces pour l'Etat, l'industrie et la société, le postulat sur lequel s'appuie la stratégie est qu'une cybersécurité réussie dépend de la collaboration entre toutes les parties prenantes.

45. En Allemagne, le concept de souveraineté technologique fait depuis plusieurs années des adeptes au sein du gouvernement. Après la révélation de l'espionnage perpétré par les Etats-Unis, la question a été mise au premier plan des débats publics et occupe aujourd'hui une grande partie du débat national sur la cybersécurité. La souveraineté technologique a également été explicitement abordée lors de la présentation du Programme numérique du gouvernement (Bendiek, 2014). Premier document de ce type en Allemagne, ce programme prévoit d'étendre l'accès à l'Internet haut débit sur tout le territoire national à l'horizon 2018, et d'accroître le rythme de création de sociétés spécialisées dans les technologies de l'information (à raison de 15 000 par an, contre 10 000 actuellement). Un aspect très important, dans le cadre du présent rapport, est que le gouvernement allemand s'intéresse spécifiquement à l'amélioration de la sécurité des données. La publication du Programme numérique a eu lieu en même temps que celle d'une nouvelle version de la loi du ministère fédéral de l'Intérieur sur la cybersécurité, dont le but est d'améliorer sensiblement en Allemagne la sécurité des systèmes faisant appel aux technologies de l'information (EurActiv, 2014a).

46. Sur le plan politique, le Conseil national de la cybersécurité – qui se situe au niveau des secrétaires d'Etat – traite des questions de cybersécurité, notamment les aspects relatifs à la politique de sécurité, économique, de défense et des affaires étrangères. Ce conseil a pour tâche de coordonner les outils de prévention ainsi que les approches interdisciplinaires de la cybersécurité mises en œuvre par les secteurs public et privé. Les réunions de ce conseil ont donc lieu en présence non seulement de la chancellerie fédérale et des représentants des *Länder* fédéraux, mais aussi d'un secrétaire d'Etat de chacun des ministères fédéraux suivants : Affaires étrangères, Intérieur, Défense, Economie et Technologies, Justice, Finances et Education et Recherche. Des représentants du monde de l'entreprise sont en outre régulièrement invités en tant que membres associés. Pour soutenir cette approche politique d'ensemble, une plateforme de coopération et d'échange d'informations – l'Alliance pour la cybersécurité – a été créée en octobre 2012. Cette alliance permet une coopération étroite entre les partenaires des milieux économiques, universitaires et administratifs, ainsi qu'avec les entreprises présentant un intérêt public particulier (Gouvernement fédéral allemand, 2014).

47. Sur le plan des services, le Bureau fédéral pour la sécurité de l'information (BSI), créé en 1991, est le principal prestataire de services de sécurité dans le domaine des technologies de l'information en Allemagne. En sa qualité d'organisme indépendant de consultation et de soutien pour la sécurité des systèmes faisant appel aux technologies de l'information, le BSI joue également le rôle de centrale de notification des incidents y afférents. Ses tâches consistent

principalement à émettre des avertissements sur les vulnérabilités des produits et services qu'offrent les technologies de l'information, à diffuser des informations auprès des parties concernées et du grand public, et à recommander des mesures de protection. Dès 1994, le BSI avait créé une CERT pour les organismes fédéraux, la « CERT-Bund ». Cette CERT nationale fonctionne comme une plateforme et un point de contact centralisé pour connaître les mesures de prévention et de réactions qu'il faut appliquer en cas d'incident lié à la sécurité informatique. Depuis 2006, une CERT citoyenne (*Bürger-CERT*) intervient auprès du grand public et des petites entreprises pour les sensibiliser aux menaces du cyberspace (Bureau fédéral allemand pour la sécurité de l'information, 2013).

48. Tout en reconnaissant qu'une cyberattaque menée contre une infrastructure de télécommunication essentielle peut causer plus de mal qu'une attaque physique, l'Allemagne maintient que le terme de « cyberguerre » est trompeur, car il suppose le scénario improbable d'une menace existentielle lancée contre un Etat par d'autres Etats par le seul biais d'attaques ciblées contre des systèmes informatiques. Dans ses lignes directrices de défense, l'Allemagne suppose au contraire que le cyberspace n'est que l'une des options utilisables par des adversaires militaires dans un contexte général de guerre. Elle considère donc le cyberspace comme un champ d'opérations militaires. Un aspect très important de ces lignes directrices est que les stratégies politico-militaires classiques sont considérées comme inadaptées face aux risques que représente le cyberspace. Des approches alternatives sont donc préconisées, l'accent étant mis sur la nécessité de renforcer la résilience aux cyber attaques, d'établir un cadre juridique clair pour l'utilisation des systèmes d'information et de communication, et favoriser un engagement national fort en faveur de mesures visant à rétablir la confiance (Gouvernement fédéral allemand, 2014).

49. S'appuyant sur le Plan national de 2005 pour la protection des infrastructures de l'information, le gouvernement fédéral a adopté en 2009 une stratégie pour la protection des infrastructures essentielles, qui prône une relation de coopération entre les autorités publiques et les opérateurs privés de ces infrastructures (Dolle, 2014). Bien que cette stratégie repose sur la volonté des entreprises de renforcer leurs niveaux de protection, le gouvernement allemand se réserve le droit de légiférer si les entreprises ne prennent pas les dispositions nécessaires. Par ailleurs, le Centre national de situation sur les technologies de l'information, géré par le BSI, se tient au courant de la situation nationale et mondiale au regard de la sécurité des systèmes de technologies de l'information. Dans l'éventualité d'une crise, ses capacités sont élargies et il devient un Centre national de réaction en cas de crise, capable d'intervenir y compris sur les réseaux et les infrastructures essentielles de l'Etat (Gouvernement fédéral allemand, 2014). La nouvelle version de la loi sur la cybersécurité propose des normes minimales pour la cybersécurité des entreprises présentant une importance vitale, ainsi qu'une obligation de rendre compte des « importants incidents de sécurité survenant sur les systèmes de technologies de l'information », en demandant aux fournisseurs d'accès Internet et aux opérateurs des réseaux de télécommunications publics qu'ils élèvent le niveau des normes de sécurité (Zeldin, 2014).

D. LE ROYAUME-UNI

50. Au Royaume-Uni, les cybermenaces sont classées au niveau un (le plus élevé) des risques pour la sécurité nationale. Le marché de l'Internet y est estimé à 82 milliards de livres sterling par an, et un pourcentage inquiétant – 93 % – des grandes entreprises ont subi une cyberattaque de leur réseau au cours du dernier exercice budgétaire (House of Commons, 2014).

51. En novembre 2011 le gouvernement britannique a publié une stratégie nationale sur la cybersécurité. Allouant une enveloppe de 860 millions de livres pour améliorer la réaction du Royaume-Uni face aux cybermenaces, cette stratégie expose la vision gouvernementale « d'un cyberspace dynamique, sûr et robuste » et définit un cadre pour « améliorer la prospérité, la

sécurité nationale et la solidité de la société » (Gouvernement britannique, 2014). Quatre objectifs clés y sont énoncés :

- s'attaquer à la cybercriminalité et faire du pays l'un des lieux les plus sûrs au monde pour mener des activités commerciales dans le cyberspace ;
- rendre le pays plus résilient aux cyberattaques et mieux préparé à protéger les intérêts nationaux dans le cyberspace ;
- créer un cyberspace ouvert, stable et dynamique, qui puisse être utilisé en toute sécurité par le grand public et qui permette le développement de sociétés ouvertes ;
- acquérir les compétences et les capacités nécessaires pour atteindre tous les objectifs en matière de cybersécurité.

Le Programme national sur la cybersécurité (NCSP) du *Cabinet Office* coordonne et finance les travaux engagés par les ministères pour mettre en œuvre les objectifs de la stratégie.

52. Du point de vue organisationnel, le Bureau de la cybersécurité et de la protection des informations (OCSIA), qui se situe au niveau du *Cabinet*, est chargé d'aider le ministre du *Cabinet Office* et le Conseil de sécurité national à définir des priorités au regard de la sécurisation du cyberspace. L'OCSIA est chargé de fournir des orientations stratégiques pour la politique gouvernementale en la matière, ainsi que d'améliorer la cybersécurité et la protection des informations au Royaume-Uni. Il collabore avec d'autres grands ministères et organismes publics tels que le *Home Office*, le ministère de la Défense (MOD), le *Government Communications Headquarters*, la Direction de la sécurité électronique/des communications, le Centre pour la protection des infrastructures nationales (CPNI), le Bureau des Affaires étrangères et du Commonwealth, ainsi que la Direction des entreprises, de l'innovation et des compétences.

53. Le CPNI fournit des conseils en matière de sécurité concernant le matériel, le personnel et les informations des infrastructures nationales essentielles. Le gouvernement britannique classe les infrastructures en fonction de l'impact que produirait leur défaut de fonctionnement. Il utilise pour cela une « échelle de mesure de l'importance vitale » qui s'appuie sur trois critères : l'impact sur la fourniture des services essentiels de la nation, l'impact économique (dû à la non-fourniture d'un service essentiel) et l'impact sur la vie humaine (dû à la non-fourniture d'un service essentiel) (CPNI, 2014). Dans la mesure où une grande partie des infrastructures britanniques sont détenues et gérées par le secteur privé, l'une des missions clés du CPNI est de fournir conseils et assistance aux entreprises présentant une importance vitale.

54. La CERT-UK a été créée fin mars 2014, suite au regroupement dans un seul cadre de gestion de l'équipe de réaction aux incidents en matière de cybersécurité et du Partenariat pour le partage des informations sur la cybersécurité (CISP). Pour encourager la coopération entre les acteurs du secteur public et de l'industrie, le CISP fonctionne comme une plateforme en ligne, en fournissant des informations sur les menaces et les incidents en matière de sécurité. Grâce à ce partenariat, les organisations participantes peuvent diffuser rapidement des informations importantes telles que des détails sur un type particulier de cyberattaque. La CERT-UK travaille en association avec d'autres CERT gouvernementales comme GovCertUK (qui aide les organisations du secteur public à réagir en cas d'incidents) et MODCERT (qui coordonne les actions du MOD lors des incidents) (Pritchard, 2013). La CERT-UK est censée coopérer avec les pouvoirs publics et l'industrie en cas d'incidents de cybersécurité survenant à l'échelle nationale. Elle tente également d'établir des partenariats avec d'autres Etats et leur CERT (comme par exemple le NCCIC américain) aux niveaux bilatéral et multilatéral, et organise des cyber exercices internationaux pour améliorer la connaissance commune des cybermenaces (Gouvernement britannique, 2014). Ainsi, le Sommet mondial sur l'innovation et la cybersécurité lancé récemment par le *Security Information Network* (SINET) a pour but d'établir des partenariats public-privé internationaux visant à améliorer la protection des infrastructures essentielles, ainsi que la défense des intérêts économiques et liés à la sécurité du Royaume-Uni et des Etats-Unis.

55. Le Partenariat pour la cyberprotection du secteur de la défense (DCPP) est, au sein du MOD, l'équivalent sur le plan organisationnel du CISP. Le secteur de la défense faisant l'objet de cyberattaques et d'incidents plus sophistiqués, le DCPP a pour mission d'accroître la sensibilisation aux cyber-risques d'un bout à l'autre de la chaîne logistique du secteur, d'améliorer la coopération entre les pouvoirs publics et l'industrie, et de permettre aux participants du secteur privé de s'aider les uns les autres grâce au partage d'informations (Pritchard, 2013). De son côté, la MOD-CERT réagit aux incidents de sécurité qui touchent les systèmes informatiques du MOD, et mène des actions pour réduire la vulnérabilité de ces systèmes aux cybermenaces. Un *Joint Forces Cyber Group* a également été créé au MOD pour accroître les capacités de défense de ce ministère dans le cyberspace.

E. L'ESTONIE

56. En 2007, l'Estonie a fait l'objet d'une cyberattaque qui, en termes d'ampleur et de cibles touchées, était sans précédent. Tous les serveurs informatiques des institutions de l'Etat, des grandes banques privées, sociétés de télécommunications, organes d'informations et autres acteurs majeurs ont, à cette époque, été visés (Davis, 2007). Si cette attaque n'a pas causé de dommage physique ni de préjudice économique majeur, elle a en revanche donné lieu à un réexamen complet de la sécurité des services électroniques de l'administration estonienne, et incité à une intensification des mesures de sécurité. Elle a également imprimé une impulsion vigoureuse aux autres Etats et organisations internationales aux fins qu'ils poursuivent leurs efforts en matière de cybersécurité.

57. La stratégie de l'Estonie en matière de cybersécurité pour 2014-2017 s'appuie sur le précédent document stratégique, qui s'appliquait à la période 2008-2013. Quatre objectifs importants ont, à cet égard, été définis (ministère estonien des Affaires économiques et de la Communication, 2014a ; 2014b) :

- mettre en place un ensemble complet de mesures pour assurer la cybersécurité à l'échelle nationale ;
- atteindre un niveau très élevé de sensibilisation et de compétence en matière de sécurité des informations ;
- Continuer à mettre au point des réglementations adaptées permettant une utilisation sûre et étendue des systèmes d'information ;
- Promouvoir la coopération internationale dans le domaine de la cybersécurité et en assumer le rôle pilote.

58. En Estonie, la coordination de la stratégie en matière de cybersécurité est assurée non plus par le MOD mais, depuis 2011, par le ministère des Affaires économiques et de la Communication (MAEC) ; la raison de ce changement est que la majeure partie des infrastructures de communication utilisées par les citoyens et les institutions de l'Etat appartiennent à des entreprises privées (Raud, 2012). Le MAEC est également chargé de réglementer les services de communication et de fournir certains services vitaux (par exemple au secteur de l'énergie), ce qui lui confère un statut unique au regard des infrastructures essentielles publiques.

59. La coopération institutionnelle est très importante en matière de cybersécurité, raison pour laquelle le MAEC collabore avec l'ensemble des autres ministères, en particulier ceux de l'Intérieur, de la Défense, des Affaires étrangères, ainsi que de l'Education et la Recherche. Une coopération approfondie s'opère également avec le Centre international d'études sur la défense (ICDS) – un organisme de recherche sur les politiques publiques – et la cyber-unité de la Ligue de défense estonienne – une organisation de défense nationale composée de volontaires. Le MAEC supervise les travaux de l'Autorité estonienne des systèmes d'information (EISA), qui met au point des stratégies et des orientations en matière de cybersécurité et contrôle la mise en œuvre

des mesures de protection des systèmes d'information et des sources de services publics essentiels. L'EISA assure la gestion de la CERT-Estonie et coopère étroitement avec d'autres CERT du monde entier en communiquant des informations sur les violations de données et en émettant des alertes relatives aux menaces liées à la sécurité.

60. Au niveau de l'Etat, la coopération entre les diverses institutions et le secteur privé est assurée par le Conseil pour la cybersécurité, créé en 2009 au sein du Comité de sécurité du gouvernement estonien (Ministère estonien des Affaires économiques et de la Communication, 2014a). Ce Conseil contrôle la mise en œuvre des objectifs énoncés dans les stratégies de l'Estonie en matière de cybersécurité. Il est présidé par le secrétaire général du MAEC.

61. La coopération nationale et internationale de l'Estonie pour l'amélioration de la cybersécurité concerne trois domaines : la protection des infrastructures et des services d'importance vitale, la cybercriminalité et la défense nationale. Ces trois domaines étant liés entre eux, le but ultime est d'assurer la continuité et la sauvegarde des processus de gouvernance, notamment la protection des infrastructures essentielles et la mise en place de solutions alternatives à l'aide de technologies innovantes. L'Estonie accorde une attention toute spéciale à l'éducation de ses citoyens et à leur sensibilisation, en particulier sur la question de la cybercriminalité.

F. L'OTAN

62. C'est au Sommet de Prague en 2002 que la cyberdéfense a été inscrite pour la première fois à l'ordre du jour politique de l'OTAN. Le sujet a ensuite suscité un intérêt majeur après les cyberattaques dont a été victime l'Estonie en 2007, puis la Géorgie en 2008 dans le cadre du conflit avec la Russie. Ces attaques ont mis en évidence la nécessité de prendre des mesures pour consolider les cyberdéfenses au sein de l'Alliance dans son ensemble ; la première politique officielle de l'OTAN sur le thème de la cyberdéfense a été adoptée en janvier 2008. Elle a été révisée en 2011 et un plan d'action pour sa mise en œuvre a été décidé par l'Alliance. On compte à l'heure actuelle quelque 600 tentatives quotidiennes d'intrusion dans les réseaux de l'OTAN, et des attaques sérieuses ont lieu toutes les trois à quatre semaines. Mis à part ces chiffres, la notion de « guerre hybride » – qui a été mise en application très récemment par la Russie en Ukraine, notamment par des actes très sophistiqués de cyberespionnage – montre à quel point il est important pour l'OTAN d'adopter une approche globale à l'égard des cyberattaques (Jones, 2014). Les ministres de la Défense des pays de l'OTAN ont, de fait, adopté lors du Sommet au Pays de Galles en 2014 une politique de cyberdéfense renforcée s'inscrivant dans le cadre de la défense collective. Il en résulte – et c'est un point très important – que les cyberattaques constituant une menace pour la sécurité des Etats et de la zone euro-atlantique pourront à l'avenir être considérées par l'Alliance comme l'équivalent d'une attaque armée classique. La déclaration du Sommet stipule donc explicitement, pour la première fois, que les cyberattaques relèvent du champ d'application de l'article 5 du Traité de Washington. Les autres points importants de la nouvelle politique de cyberdéfense de l'OTAN sont notamment la détermination à appliquer le droit international au cyberspace, l'intensification de la coopération de l'OTAN avec les acteurs de l'industrie, et le développement d'une capacité OTAN utilisable dans le cyberspace.

63. L'axe central de la politique de cyberdéfense de l'OTAN est la protection des systèmes d'information et de communication lui appartenant : les réseaux installés à son siège, dans ses agences et sur le lieu de ses missions à l'étranger. L'objectif principal de l'OTAN est donc d'améliorer la prévention des attaques et la robustesse des systèmes, mais aussi d'éviter la duplication de ses efforts avec ceux déployés au niveau national ou multinational. La mission de cyberdéfense est confiée au Centre technique de la capacité OTAN de réaction aux incidents informatiques (NCIRC), qui a bénéficié d'une enveloppe de 58 millions d'euros pour moderniser ses services et est pleinement opérationnel depuis mai 2014. Le NCIRC a pour mission de fournir une protection renforcée aux réseaux de l'OTAN et à leurs utilisateurs. Il forme par exemple des équipes de réaction rapide, capables d'intervenir sur les réseaux faisant l'objet d'une attaque dans

un délai de cinq heures. Cela veut donc dire que dans les procédures actuelles de demande par les Etats membres de déploiement de ces équipes, les consultations politiques ralentissent le processus décisionnel et risquent de rendre irréalisable l'objectif d'une réaction efficace de l'OTAN en cas de cyberattaque contre un Allié (Jordan, 2014). Dans le cas d'une cyberattaque, le Conseil de l'Atlantique Nord décidera au cas par cas de l'invocation de l'article 5 du Traité. L'OTAN maintient en fait une « ambiguïté stratégique » et une flexibilité sur la question des moyens à employer pour réagir aux différents types de crises survenant dans le cyberspace. Un aspect très important est que l'Alliance n'a pas spécifié quels types d'attaques justifieraient l'invocation de la clause de défense collective, ni quelle forme prendrait la riposte.

64. D'un autre côté, l'Alliance est consciente de la dimension planétaire du cyberspace et des menaces qui y sont associées, et ne limite pas sa politique de cyberdéfense à la seule protection de ses réseaux. L'OTAN est dans une certaine mesure extrêmement dépendante des systèmes et des réseaux d'information de certains de ses pays membres, raison pour laquelle elle travaille en collaboration avec eux pour mettre au point des exigences minimales en matière de cyberdéfense. L'OTAN continuera par ailleurs à jouer un rôle de facilitatrice et à fournir un cadre d'assistance mutuelle entre les Alliés – consistant principalement à partager des informations et des bonnes pratiques. Afin que chacun des Alliés puisse renforcer ses propres capacités de cyberdéfense et contribuer à la sécurité globale de l'Alliance, le développement de capacités de cyberdéfense a été intégré au Processus de planification de la défense de l'OTAN. L'Alliance a également intégré la cyberdéfense dans de nombreux exercices ayant lieu à tous les niveaux, notamment stratégique et sur le terrain.

65. La cyberdéfense a également été intégrée à l'Initiative OTAN de défense intelligente, et plusieurs projets collaboratifs visant à préserver et développer les capacités des Alliés ont été lancés, parmi lesquels la plateforme *Malware Information Sharing*, *Smart Defence Multinational Cyber Defence Capability Development* et le projet multinational d'éducation et de formation sur la cyberdéfense. S'agissant à cet égard du volet éducatif, l'Ecole des systèmes d'information et de communication de l'OTAN, installée à Latina en Italie (qui déménagera à Oeiras au Portugal en 2016 et deviendra l'Ecole des systèmes d'information et de communication et de la cyberdéfense), l'Ecole de l'OTAN à Oberammergau en Allemagne, ainsi que le Collège de défense de l'OTAN basé à Rome délivrent des formations sur la cyberdéfense (OTAN, 2014). Le cyberpartenariat OTAN-industrie, avalisé lors du Sommet au Pays de Galles et récemment mis en place, permettra de renforcer les relations avec l'industrie. L'objectif premier de ce partenariat sera de faciliter l'accès aux innovations technologiques et à l'expertise du secteur privé. Il réunira des entités de l'OTAN, des CERT nationales et des représentants de l'industrie des pays alliés.

66. Au niveau multinational, l'OTAN et ses différents membres travaillent en collaboration avec des partenaires, des organisations internationales, des universitaires et des entités privées dans le but de promouvoir la complémentarité et d'éviter les doublons. Le Centre d'excellence pour la cyberdéfense en coopération (CCD COE), implanté à Tallinn (Estonie) et homologué par l'OTAN, est un bon exemple de la mise en pratique de la collaboration précitée. Les centres d'excellence homologués par l'OTAN ne font pas partie de la structure de commandement de l'Alliance, mais sont des organisations militaires internationales qui lui apportent leur soutien. Spécialisé dans la formation et la recherche-développement, le CCD COE se destine à devenir la principale source d'expertise dans le domaine de la cyberdéfense collaborative au sein de l'Alliance et de ses partenariats. Sur invitation du CCD COE, un groupe international d'experts a élaboré le manuel de Tallinn sur le droit international applicable à la cyberguerre (*Tallinn Manual on the International Law Applicable to Cyber Warfare*), qui est l'étude la plus complète sur le sujet en accès libre. Ce manuel devrait être suivi par un second volume qui expliquera « les possibilités dont disposent les Etats, en vertu du droit international, pour réagir aux cyberattaques d'autres pays » (Hale, 2014b). Le CCD COE organise également chaque année un exercice de défense du réseau en temps réel, baptisé *Locked Shields*. En mars 2014, cet exercice a rassemblé près de 300 participants de 17 pays, signe de la préoccupation croissante des Alliés à l'égard de la cybersécurité, ainsi que du rôle crucial du CCD COE (Apps, 2014).

67. Si le rôle de l'OTAN en matière de cyberdéfense et de protection des réseaux militaires est clair, celui concernant la défense des infrastructures essentielles contre les cybermenaces n'est pas vraiment défini. En tant qu'alliance politico-militaire intergouvernementale, l'OTAN n'est pas habilitée à gérer les infrastructures civiles ou privées. Sa stratégie en matière de cyberdéfense souligne l'importance de la coopération avec les Alliés pour mettre au point des exigences minimales applicables aux systèmes et réseaux d'information nationaux d'importance vitale qui sont connectés à l'OTAN ou traitent des informations OTAN essentielles pour les tâches fondamentales de celle-ci. Cela dit, au-delà d'une assistance pour renforcer les capacités de cyberdéfense à l'égard de ces systèmes et ces réseaux, l'OTAN n'est pas habilitée à élaborer une stratégie concernant la protection des infrastructures essentielles. Elle a néanmoins conscience de la gravité des conséquences éventuelles d'une cyberattaque coordonnée contre des infrastructures essentielles, et certains appellent à ce qu'elle réfléchisse au rôle qu'elle pourrait jouer pour protéger ces infrastructures. La conférence OTAN de 2012 sur les défis de sécurité émergents en Europe, a par exemple conclu que « l'OTAN doit participer, au côté d'autres parties prenantes, au débat concernant la façon de procéder pour évaluer les vulnérabilités de première gravité, fournir des formations et un enseignement, et comprendre/prévenir les menaces » (Division Défis de sécurité émergents de l'OTAN, 2012). Tandis que le CCD COE de Tallinn mène à cet égard des travaux constructifs, l'OTAN n'en est encore qu'aux prémices d'une réflexion sur le rôle qu'elle pourrait jouer au regard de la protection des infrastructures essentielles contre les cybermenaces. S'agissant des Alliés européens, la cyberprotection des secteurs d'importance vitale sera bientôt régie par une réglementation de l'UE ayant trait à la sécurité des réseaux et de l'information (ou Directive SRI, voir plus bas).

G. L'UNION EUROPEENNE

68. La Commission européenne, associée à la Haute Représentante de l'UE pour les Affaires étrangères et la Politique de sécurité, a publié le 7 février 2013 la stratégie de cybersécurité de l'UE. Sous-titrée « Un cyberspace ouvert, sûr et sécurisé », cette stratégie s'applique aux réseaux tant publics que privés et a pour but de « préserver un environnement en ligne offrant le degré de liberté et de sécurité le plus élevé possible dans l'intérêt de tous » (Commission européenne, 2013a). Tout en reconnaissant que « c'est aux Etats membres qu'il incombe en premier lieu de traiter les problèmes de sécurité dans le cyberspace », ce document propose toutes sortes d'actions et d'outils stratégiques impliquant les institutions européennes, les Etats membres et les entreprises privées, dans le but d'améliorer les performances globales de l'UE. La vision de l'UE exposée dans cette stratégie s'articule autour de cinq priorités :

- parvenir à la cyber-résilience ;
- faire reculer considérablement la cybercriminalité ;
- développer une politique et des moyens de cyberdéfense liés à la politique de sécurité et de défense commune (PSDC) ;
- développer les ressources industrielles et technologiques en matière de cybersécurité ;
- instaurer une politique internationale de l'Union européenne cohérente en matière de cyberspace et promouvoir les valeurs essentielles de l'UE.

69. Bien qu'une seule des cinq priorités ci-dessus concerne spécifiquement le secteur de la défense, dans la mesure où les cybermenaces sont souvent multiformes, il est entendu qu'« il faut développer des synergies entre les approches civile et militaire de la protection des cyberinfrastructures critiques » (Commission européenne, 2013a). En définitive, l'UE en est au début de la conception et de la mise en œuvre d'une stratégie globale en matière de cybersécurité. La situation devrait considérablement progresser en 2014-2015, avec l'adoption de la Directive SRI – en cours de négociation –, qui vise à garantir un niveau élevé et commun de sécurité des réseaux et de l'information au sein de l'UE. Cette directive aura plus particulièrement pour objectif :

- d'aider les Etats membres à mettre au point des politiques, des organisations et des capacités nationales pour réagir face à la cybermenace (mise en place d'une CERT nationale, définition d'une stratégie en matière de cybersécurité) ;
- de mettre en place des mesures importantes pour renforcer la cyberprotection des infrastructures d'importance vitale au sein de chaque Etat membre (obligation de notification, mesures de sécurité minimales) ;
- de fournir un cadre de coopération durable entre les Etats membres, tant sur le plan politique qu'opérationnel.

70. De manière plus générale, l'objectif de l'UE est de réduire les vulnérabilités des infrastructures essentielles et d'accroître leur résilience, de manière à limiter autant que possible « les effets néfastes des perturbations pour la société et les citoyens » (Commission européenne, DG Affaires intérieures, 2013). La protection des infrastructures essentielles vise donc tous les types de menaces et de risques, dont la cybermenace. Le document de travail de la Commission sur une nouvelle approche du programme européen de protection des infrastructures critiques (août 2013) simplifie la politique en vigueur dans trois domaines : prévention, préparation et réaction. La stratégie de cybersécurité de l'UE y est décrite comme une source « d'actions qui favoriseront une meilleure cyber-résilience et une plus grande protection des infrastructures concernées [par le programme européen de protection des infrastructures critiques] » (Commission européenne, 2013b).

71. S'agissant de la PSDC, le Conseil européen a, en 2013, appelé à l'élaboration d'un cadre d'action de l'UE en matière de cyberdéfense. Ce cadre, qui sera préparé par la Haute Représentante de l'UE pour les Affaires étrangères et la Politique de sécurité, en collaboration avec la Commission et l'Agence européenne de défense (AED), a pour but de favoriser (Conseil de l'Europe, 2013) :

- « le développement des capacités de cyberdéfense des Etats membres, de la recherche et des technologies grâce à l'élaboration et à la mise en œuvre d'une feuille de route globale pour le renforcement des capacités en matière de cyberdéfense ;
- le renforcement de la protection des réseaux de communication au service des structures, missions et opérations dans le cadre de la PSDC ;
- l'intégration de la cybersécurité dans la gestion des crises de l'UE ;
- la sensibilisation grâce à l'amélioration des possibilités de formation, d'éducation et d'exercice offertes aux Etats membres ;
- le développement de synergies avec des cyberpolitiques plus générales de l'UE et tous les autres acteurs et agences compétents en Europe, tels que l'Agence de l'UE chargée de la sécurité des réseaux et de l'information ;
- la coopération avec les partenaires internationaux pertinents, notamment l'OTAN, le cas échéant. »

72. La politique de l'UE relative à la protection des réseaux des Etats membres associés à la sécurité nationale et aux institutions militaires est donc conçue comme un cadre favorisant la collaboration entre les gouvernements nationaux et l'AED, en coordination avec la PSDC. L'UE reconnaît cependant « qu'un cyberincident ou une cyberattaque particulièrement grave pourrait constituer un motif suffisant pour qu'un Etat membre invoque la clause de solidarité de l'UE ».

73. Les organisations de l'UE telles que l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) et la CERT des institutions européennes (CERT-EU) ont pour but de coordonner et soutenir les activités nationales. Ainsi, dans le but de faciliter la coopération et la coordination, l'ENISA a encouragé chaque Etat membre à créer, avec le soutien gouvernemental, une seule CERT nationale ; elle a également publié un ensemble de normes minimales en matière de capacités que les Etats sont tenus de respecter (Pritchard, 2013). En avril 2014, l'ENISA a invité plus de 200 organisations (dont des compagnies énergétiques, des

opérateurs de télécommunications et des professionnels de la sécurité) à participer à Cyber Europe 2014, un exercice visant à déterminer comment les Etats peuvent, ensemble, lutter contre une menace transfrontière de grande ampleur (Hale, 2014a). De manière générale, l'UE vise, via l'ENISA, à fournir à ses Etats membres un cadre d'échange d'informations et de bonnes pratiques sur la cybersécurité.

74. La CERT-EU a été créée en 2012 pour fournir aux institutions, organes et agences de l'UE une capacité commune en matière de défense des réseaux. Son rôle est donc d'aider les institutions de l'UE en cas d'atteinte à la cybersécurité. La CERT-EU n'est pas habilitée à coordonner ou soutenir les activités menées à l'échelle nationale. Elle est l'équivalent, à l'UE, du NCIRC de l'OTAN.

IV. CONCLUSION

75. Les menaces à la sécurité nationale provenant du cyberespace sont une grave préoccupation pour l'ensemble des pays qui font une utilisation massive des réseaux et systèmes informatiques. Les formes les plus graves de criminalité, de terrorisme, d'espionnage et de sabotage cybernétiques, voire les cyberattaques commises par des acteurs étatiques, feront partie du paysage courant de l'environnement stratégique futur. Toutes les initiatives militaires incluront à l'avenir des cybercapacités. Ces difficultés confèrent à la gestion de la sécurité internationale un niveau de complexité totalement inédit. Elles ne sont toutefois pas aussi insurmontables que le prétendent certains, si tant est que les gouvernements et les propriétaires/opérateurs des infrastructures essentielles déploient tous les efforts nécessaires. Une bonne cyberdéfense doit être le fondement des stratégies nationales. Sans cela, la cyberdissuasion et l'éventuelle maîtrise des cyberarmes ne fonctionneront pas. Dans le contexte du cyberespace, la dissuasion et la maîtrise des armes continuent de poser aux responsables politiques de nombreuses et difficiles questions. Il conviendra d'y répondre si l'on veut consolider les efforts en matière de cybersécurité. En fait, la priorité doit être, pour chaque Etat, de se concentrer d'abord sur la cyberdéfense puis, lorsqu'un niveau durable aura été atteint à cet égard, de s'orienter s'il le souhaite vers la mise en place de cybercapacités offensives et la maîtrise des cyberarmes.

76. Les efforts en matière de cybersécurité sont avant tout une responsabilité nationale que les Etats doivent endosser. Cela est particulièrement vrai au sein d'une alliance, car les cybermenaces ne connaissent pas de frontières. Il existe, à l'heure actuelle, des écarts importants entre les capacités de cyberdéfense dont disposent les différents pays membres de l'OTAN. A moyen ou long terme, cela peut avoir de graves conséquences et crée, de fait, une situation intenable : une attaque prenant pour cibles des Alliés possédant peu de capacités en matière de cybersécurité peut avoir des effets désastreux sur les Alliés qui ont, eux, beaucoup investi dans le domaine. Une cybermenace visant l'un des pays de l'OTAN pourrait donc porter préjudice à l'ensemble des Alliés. Il est, par conséquent, impératif que tous les Alliés continuent à accroître leur cybersécurité au niveau national. L'intégration en cours des capacités de cyberdéfense dans le Processus de planification de la défense de l'OTAN est, à cet égard, une bonne nouvelle. A mesure que les initiatives nationales suivent leur cours, la coopération internationale – notamment dans le cadre de l'OTAN et de l'UE – présente un important potentiel encore inconnu et inexploité. En 2014, l'OTAN a mis au point une stratégie en matière de cyberdéfense et l'UE est en train de faire de même ; ces stratégies permettront d'améliorer notre sécurité collective et individuelle. Les délais de réaction étant d'une importance cruciale en cas de cyberattaque, les Etats membres de l'Alliance et de l'UE devraient s'efforcer de simplifier les processus de décision des instances politiques, afin que l'application au cyberespace des principes de défense collective soit pleinement efficace. Il serait toutefois prématuré, à ce stade, de confier davantage de prérogatives à l'une ou l'autre de ces deux organisations. D'une part, tous les pays ne sont pas égaux en matière de cyberdéfense mais, surtout, la coopération en la matière est encore très complexe étant donné que la cybersécurité est une composante nouvelle de la politique de défense des

pays. Le renforcement de la coopération ne devra avoir lieu que lorsque les autorités nationales auront compris la cybermenace et conçu des politiques internes cohérentes. Il serait donc préférable que les Etats soient davantage incités à accroître leur cyberdéfense, pour le bien de tous. Les stratégies de l'OTAN, de l'UE et des différents pays doivent être étroitement coordonnées, non seulement pour éviter la duplication des efforts, mais aussi parce qu'il est en fait difficile de coordonner les stratégies sur une question qui dépasse souvent les frontières nationales et régionales. La cybermenace n'est pas vouée à disparaître, et les législateurs de l'Alliance doivent comprendre les difficultés de l'énorme défi que représente l'intégration de la cyberdéfense dans les politiques nationales et internationales de la défense.

BIBLIOGRAPHIE

- ANSSI, *Missions*, 2013, <http://www.ssi.gouv.fr/fr/anssi/missions/>
- Apps, Peter, « Estonia Exercise Shows NATO's Growing Worry about Cyber-Attacks », *Reuters*, 27 mai 2014, <http://www.reuters.com/article/2014/05/27/us-nato-cybercrime-exercise-idUSKBN0E729V20140527>
- Bendiek, Annegret, *Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance and Data Protection*, Berlin: Stiftung Wissenschaft und Politik, 2014
- Betz, David J et Tim Stevens, « Chapter Three: Cyberspace and War », *Adelphi Series*, n° 51, 2011.
- Bockel, Jean-Marie, « Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense », *Rapport du Sénat de la République française*, n° 681, 2012.
- Bureau fédéral allemand pour la sécurité de l'information, « IT Crisis Management ». *CERT Bund*, 14 juillet 2013, https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/Cert-Bund/cert-bund_node.html
- Commission européenne (DG Affaires intérieures), *Critical Infrastructure*, 29 novembre 2013, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm
- Commission européenne, *Stratégie de cybersécurité de l'Union européenne : un cyberspace ouvert, sûr et sécurisé*, JOIN(2013) 1 Final, 2013a.
- Commission européenne, *On a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure*, SWD(2013) 318 final, 2013b
- Conseil de l'Europe, "Council Conclusions on Common Security and Defence Policy," Education, Youth, Culture and Sport Council Meeting, 25-26 novembre 2013
http://www.eeas.europa.eu/top_stories/pdf/20131126_council_conclusions_en.pdf
- CPNI, « The national infrastructure », *Centre for the Protection of National Infrastructures*, 2014, <http://www.cpni.gov.uk/about/cni/>
- CSIS/McAfee, *The Economic Impact of Cybercrime and Cyber Espionage*, CSIS, 2013, <http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf>
- Davis, Joshua, « Hackers Take Down the Most Wired Country in Europe », *Wired*, vol. 15, n° 9, 2007
- Division Défis de sécurité émergents de l'OTAN, *The World in 2020 – Can NATO Protect Us*, 2012, http://lgdata.s3-website-us-east-1.amazonaws.com/docs/1494/764045/ESC_Conference_2012_12_10_FINAL.pdf.
- Dolle, Wilhelm, *IT Sicherheit in Deutschland: Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes*, Berlin: KPMG, 2014
- Drinkwater, Doug, « France Working To Protect Critical Infrastructure From Cyber Attacks », *SC Magazine*, 12 août 2014, <http://www.scmagazineuk.com/france-working-to-protect-critical-infrastructure-from-cyber-attacks/article/365844/>
- EurActiv, « *German Digital Agenda Is 'Better Late Than Never'* », *EurActiv*, 21 août 2014, 2014a, <http://www.euractiv.com/sections/innovation-enterprise/german-digital-agenda-better-late-never-307876>
- EurActiv, « Robert Madelin: EU 'Not Putting Its Money Where Its Mouth Is' On Broadband », *EurActiv*, 5 septembre 2014, 2014b, <http://www.euractiv.com/sections/innovation-enterprise/robert-madelin-eu-not-putting-its-money-where-its-mouth-broadband>
- Fagan, David, Richard Hertling, et Sumon Dantiki, « House of Representatives Passes Three Cybersecurity Bills », *Inside Privacy*, 30 juillet 2014, <http://www.insideprivacy.com/uncategorized/house-of-representatives-passes-three-cybersecurity-bills/>
- Farwell, James P et Rafal Rohozinski, « The New Reality of Cyber War », *Survival*, vol. 54, n° 4, 2012.
- Gouvernement britannique, *Developments In The Field of Information And Telecommunications In The Context Of International Security: UK Submission*, New York: United Nations Office of Disarmament, 2014
- Gouvernement fédéral allemand, *Developments in the Field of Information and Telecommunications in the Field of International Security: German Submission*, New York: United Nations Office of Disarmament, 2014
- Gray, Colin S, *Making Strategic Sense of Cyber Power: Why the Sky is not Falling*, Carlisle, U.S. Army War College Press, 2013.
- Hale, James, « Game Theory: Cyber Preparedness », *SC Magazine*, 2 septembre 2014, 2014a, <http://www.scmagazine.com/game-theory-cyber-preparedness/article/366363/>
- Hale, Julian, « NATO-backed Project Explores Legal Options to Respond to Cyberattacks », *Defense News*, 23 janvier 2014, 2014b,

- <http://www.defensenews.com/article/20140123/DEFREG04/301230033/NATO-backed-Project-Explores-Legal-Options-Respond-Cyberattacks>
- House of Commons, *Parliamentary Debates (Hansard)*, London: House of Commons Official Reports, 2014
- Jones, Sam, « Ukraine: Russia's New Art of War », *Financial Times*, 28 août 2014, <http://www.ft.com/intl/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html#axzz3EDhkd7a>
- Jordan, Klara Tothova, « NATO Must Boost Its Cyber Defense Capabilities Now », *Atlantic Council*, 12 septembre 2014, <http://www.atlanticcouncil.org/blogs/natosource/nato-must-boost-its-cyber-defense-capabilities-now>
- Joubert, Vincent, « Les Budgets Nationaux De Cyberdefense En Croissance Constante », *Défense&Industries*, n° 1, 2014
- Krayem, Norma M, Ludmilla L Savelief, Amy F Davenport, et Samantha A Martin, « The Congress Ramps Up Action On Cybersecurity Legislation Possibilities For Data Protection/Breach Legislation Still Exist », *Lexology*, 5 septembre 2014, <https://www.lexology.com/library/detail.aspx?g=c0aef159-afe5-45c4-a12b-2a784e01e595>
- Kuehl, Daniel F, « From Cyberspace to Cyberpower: Defining the Problem », in Kramer, Franklin D, Stuart H Starr, et Larry K Wentz (dir. pub.), *Cyberpower and National Security*, Washington, DC, National Defense University Press, 2009.
- Libicki, Martin C, *Cyberdeterrence and Cyberwar*, Santa Monica, RAND Corporation, 2009.
- Lin, Herbert S, « A Virtual Necessity: Some Modest Steps Toward Greater Cybersecurity », *Bulletin of the Atomic Scientists*, vol. 68, n° 5, 2012.
- Lin, Herbert S, « Offensive Cyber Operations and the Use of Force », *Journal of National Security Law & Policy*, vol. 4, n° 63, 2010.
- Maison-Blanche, 2010 *National Security Strategy*, 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
- Maison-Blanche, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- Département américain de la Défense, *Department of Defense Strategy for Operating in Cyberspace*, 2011, <http://www.defense.gov/news/d20110714cyber.pdf>
- Département américain de la Sécurité intérieure, *Critical Infrastructure Security*, n.d., <https://www.dhs.gov/topic/critical-infrastructure-security>
- Protection Making European Critical Infrastructures More Secure*, SWD(2013) 318 final, 2013b
- Ministère estonien des Affaires économiques et de la Communication, « Cyber security », 2014, 2014a <https://www.mkm.ee/en/objectives-activities/information-society/cyber-security>
- Ministère estonien des Affaires économiques et de la Communication, « Küberjulgeoleku strateegia 2014-2017 », 2014b. https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf
- Ministère fédéral allemand de la Défense, *Germany: Defence Policy Guidelines 2011 Safeguarding National Interests – Assuming International Responsibility – Shaping Security Together*, Berlin, Defense White Papers and National Security Strategies, 2011
- OTAN, *Cyber Defence*, 30 Septembre 2014, http://www.nato.int/cps/en/natohq/topics_78170.htm?
- Pritchard, Robert, « UK Cyber Response - Getting It Right Matters », *RUSI Analysis*, 30 septembre 2013, https://www.rusi.org/go.php?structureID=commentary&ref=C52497E7E68AB2#.VCu_8Gd_tqV
- Raud, Helen, « Cyber Security », *Estonian Information Society Yearbook 2011/2012*, 2012, Estonia State Information Systems (RISO), http://www.riso.ee/sites/default/files/info%C3%BChiskonna%20aastaraamat_2011_ENG_FINAL_0.pdf
- République française, *Livre blanc sur la défense et la sécurité nationale*, 2013, http://www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf
- Rid, Thomas, « *Cyber War will not take place* », Oxford University Press, 2013
- Robinson, Neil, « Tangled Web: Cybersecurity Strategies Raise Hopes of International Cooperation », *RAND Review*, été 2013.
- Robinson, Neil, Luke Gribbon, Veronika Horvath, and Kate Robertson, *Cyber-Security Threat Characterisation: A Rapid Comparative Analysis*, Santa Monica: RAND, 2013
- Romm, Tony, « Cybersecurity in Slow Lane One Year after Obama Order », *Politico*, 9 février 2014, <http://www.politico.com/story/2014/02/cybersecurity-in-slow-lane-one-year-after-obama-order-103307.html>
- Selyukh, Alina, « U.S. to Offer Companies Broad Standards to Improve Cybersecurity », *Reuters*, 12 février 2014, <http://www.reuters.com/article/2014/02/12/us-usa-cybersecurity-standards-idUSBREA1B0AL20140212>

Serbu, Jared, « National Guard Carves Out Its Slice Of Dod Cyber Mission, Wants Teams In Every State », *Federal News Radio*, 3 septembre 2014, <http://www.federalnewsradio.com/396/3693882/National-Guard-carves-out-its-slice-of-DoD-cyber-mission-wants-teams-in-every-state>

Zeldin, Wendy, "Germany: Ministry of the Interior Publishes Draft Cybersecurity Act," *Global Legal Monitor*, 10 septembre 2014, http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205404116_text
